WHAT IS CLAIMED IS:

~~Sub~~ ~~a1~~ a1

Sub D1

1. A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data.

2. The method of claim 1, wherein the signing step comprises:

applying a one-way hashing function to the digital data excluding said predetermined bits resulting in a hash; and encrypting the hash.

3. The method of claim 1, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

4. The method of claim 1, further comprising the step of inserting associated data into the digital data prior to the signing step such that the digital signature authenticates both the associated data as well as the digital data.

a 5. The method of claim ~~4~~ 1, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

a 6. The method of claim ~~4~~ 1, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the predetermined bits comprise at least a portion of the least significant bit plane.

7. The method of claim 6, wherein the digital data is an image and each sample is an image pixel.

8. The method of claim 6, wherein the digital data is video and each sample is a spatial temporal sample.

9. The method of claim 6, wherein the digital data is audio and each sample is a time sample.

10. The method of claim 6, wherein the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

b 11. The method of claim ~~4~~ 1, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, further comprising the step of transforming the plurality of bits into an alternative representation having at least first and second characteristic components, wherein the predetermined bits comprise the first characteristic component.

12. The method of claim 11, wherein the digital data is an image and each sample is an image pixel.

13. The method of claim 11, wherein the digital data is video and each sample is a spatial temporal sample.

14. The method of claim 11, wherein the digital data is audio and each sample is a time sample.

15. The method of claim 11, wherein the associated data is inserted into at least a portion of the second characteristic component.

16. The method of claim 15, wherein the alternative representation is a frequency domain representation having high and low frequency components, wherein the first characteristic component is a portion of the high frequency component and the second characteristic component is the remaining high frequency component and the low frequency component.

~~17. The method of claim 4, wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature.~~

18. The method of claim 1 ~~4~~, wherein the associated data comprises data identifying a source of the digital data.

19. The method of claim 1 ~~4~~, wherein the associated data comprises data identifying the identity of an owner of the digital data.

20. The method of claim 19, wherein the digital data is an image and the associated data comprises data identifying a photographer of the image.

21. The method of claim ~~1~~ 11, wherein a portion of the associated data is encrypted and a remaining portion of the associated data is unencrypted.

22. The method of claim ~~1~~ 11, wherein the associated data comprises at least two fields.

23. The method of claim 22, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

24. The method of claim 23, wherein at least one other field comprises data identifying the owner of the public key.

25. The method of claim ~~1~~ 11, further comprising the step of receiving the associated data from an external source.

26. The method of claim 25, wherein the external source is a Global Positioning Satellite transmission.

27. The method of claim 1, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the method further comprises the steps of:

creating a decompressed file prior to the signing step; signing the decompressed file resulting in the digital signature; and inserting the digital signature into a header in the compressed file instead of inserting the same into the digital data.

28. The method of claim 27, wherein the digital data is an image and the compression standard is JPEG.

29. The method of claim 27, wherein the digital data is video and the compression standard is MPEG.

30. The method of claim ~~4~~ 1, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the method further comprises the steps of:

creating a decompressed file prior to the signing step;

inserting the associated data into the decompressed file;

signing the decompressed file resulting in the digital signature; and

inserting the digital signature and associated data into a header in the compressed file instead of inserting the same into the digital data.

31. The method of claim 30, wherein the digital data is an image and the compression standard is JPEG.

32. The method of claim 30, wherein the digital data is video and the compression standard is MPEG.

a

33. The method of claim ~~4~~ 1, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the method further comprises the steps of:

ignoring the least significant bit plane in the digital data;

concatenating the associated data to the digital data having the ignored least significant bit plane prior to the signing step;

performing the signing step to the digital data having concatenated associated data resulting in the digital signature;

wherein the predetermined bits comprise at least a portion of the least significant bit plane and the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

34. The method of claim 1, further comprising the steps of:

providing time data identifying the time the digital data was created;

concatenating the hash and the time data;

applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; and encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated.

35. The method of claim 34, further comprising the steps of:

transmitting the hash and signature to a third party for performance of the providing, concatenating, and encrypting steps; and

receiving the time stamp from the third party prior to the inserting step.

36. The method of claim 35, wherein the trusted third party resides at an internet address and the transmitting and receiving steps are done through the internet.

37. The method of claim 34, wherein the time stamp is provided by a semiconductor chip having a tamper resistant clock and a tamper resistant time stamping circuit, wherein the clock outputs the time data which together with the digital signature is signed by the circuit to output the time stamp.

38. The method of claim ~~4~~ 1, further comprising the steps of:

storing an identifier in a memory corresponding to each of at least one user of a device which creates the digital data;

recognizing a user of the device whose identifier is stored in the memory; and

outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

39. The method of claim 38, further comprising the steps of storing a private key for signing the digital data in the memory corresponding to each user and using the private key for signing the digital data.

40. The method of claim 38, wherein the recognizing step is accomplished by a fingerprint recognition system.

41. The method of claim 38, wherein the identifier is a name of the recognized user.

42. A method for authenticating digital data having an embedded digital signature in predetermined bits of the digital data, the method comprising the steps of:

extracting the digital signature from the predetermined bits;

decrypting the digital signature from the digital data resulting in a first hash;

applying a one-way hashing function used by an encoder of the digital data to the digital data excluding the predetermined bits resulting in a second hash; and comparing the first hash to the second hash wherein if the first hash matches the second hash the digital data is authentic.

43. The method of claim 42, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

44. The method of claim 42, wherein the digital data further comprises associated data inserted into known bits of the digital data, wherein the method authenticates both the associated data as well as the digital data.

45. The method of claim 44, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

46. The method of claim 44, wherein the digital data is compressed using a compression standard resulting in a compressed file and wherein the digital signature and associated data are contained in a header in the compressed file, wherein the method further comprises the steps of:

decompressing the compressed file; and

replacing the signature and associated data from the header into the predetermined bits and the known bits, respectively, prior to the extracting step.

47. An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder ~~comprising:~~

~~means for assigning predetermined bits of the digital data for receiving the digital signature;~~

~~means for signing the digital data excluding the predetermined bits resulting in the digital signature; and~~

~~means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data.~~

48. The encoder of claim 47, wherein the means for signing comprises:

means for applying a one-way hashing function to the digital data excluding said predetermined bits resulting in a hash; and

encrypting the hash.

49. The encoder of claim 47, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

~~50. The encoder of claim 47, further comprising means for inserting associated data into the digital data prior to signing the digital data such that the encoder authenticates both the associated data as well as the digital data.~~

51. The encoder of claim 47 ~~50~~, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

52. The encoder of claim 47 ~~50~~, wherein the digital data comprises a plurality of samples, each of the samples being

defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the predetermined bits comprise at least a portion of the least significant bit plane.

53. The encoder of claim 52, wherein the digital data is an image and each sample is an image pixel.

54. The encoder of claim 52, wherein the digital data is video and each sample is a spatial temporal sample.

55. The encoder of claim 52, wherein the digital data is audio and each sample is a time sample.

56. The encoder of claim 52, wherein the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

57. The encoder of claim ~~50~~ 47, wherein the digital data is an image comprising a plurality of samples, each of the samples being defined by a plurality of the bits, further comprising means for transforming the plurality of bits into an alternative representation having at least first and second characteristic components, wherein the predetermined bits comprise the first characteristic component.

58. The encoder of claim 57, wherein the digital data is an image and each sample is an image pixel.

59. The encoder of claim 57, wherein the digital data is video and each sample is a spatial temporal sample.

60. The encoder of claim 57, wherein the digital data is audio and each sample is a time sample.

61. The encoder of claim 57, wherein the associated data is inserted into at least a portion of second characteristic component.

62. The encoder of claim 61, wherein the alternative representation is a frequency domain representation having high and low frequency components, wherein the first characteristic component is a portion of the high frequency component and the second characteristic component is the remaining high frequency component and the low frequency component.

~~63. The encoder of claim 50, wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature.~~

w 64. The encoder of claim ~~50~~ 47, wherein the associated data comprises data identifying a source of the digital data.

w 65. The encoder of claim ~~50~~ 47, wherein the associated data comprises data identifying the identity of an owner of the ~~digital data.~~

B5

~~66. The encoder of claim 65, wherein the digital data is an image and the associated data comprises data identifying a photographer of the image.~~

w 67. The encoder of claim ~~50~~ 47, wherein a portion of the associated data is encrypted and a remaining portion of the associated data is unencrypted.

68. The encoder of claim ~~50~~ 47, wherein the associated data comprises at least two fields.

69. The encoder of claim 68, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

70. The encoder of claim 69, wherein at least one other field comprises data identifying the owner of the public key.

71. The encoder of claim 65, further comprising means for receiving the associated data from an external source.

72. The encoder of claim 71, wherein the external source is a Global Positioning Satellite transmission.

73. The encoder of claim 47, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the encoder further comprises:

means for creating a decompressed file prior to signing the digital data;

means for signing the decompressed file resulting in the digital signature; and

means for inserting the digital signature into a header in the compressed file instead of inserting the same into the digital data.

74. The encoder of claim 73, wherein the digital data is an image and the compression standard is JPEG.

75. The encoder of claim 73, wherein the digital data is video and the compression standard is MPEG.

76. The encoder of claim ~~50~~ 47, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the encoder further comprises:

means for creating a decompressed file prior to signing the digital data;

means for inserting the associated data into the decompressed file;

means for signing the decompressed file with the associated data inserted therein resulting in the digital signature; and

means for inserting the digital signature and associated data into a header in the compressed file instead of inserting the same into the digital data.

77. The encoder of claim 76, wherein the digital data is an image and the compression standard is JPEG.

78. The encoder of claim 76, wherein the digital data is video and the compression standard is MPEG.

79. The encoder of claim ~~50~~ 47, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the encoder further comprises:

means for ignoring at least a portion of the least significant bit plane in the digital data;

means for concatenating the associated data to the digital data having the ignored least significant bit plane prior to signing the digital data;

means for signing the digital data having the concatenated associated data resulting in the digital signature;

wherein the predetermined bits comprise at least a portion of the least significant bit plane and the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

W

80. The encoder of claim ~~50~~ 47, further comprising:

means for providing time data identifying the time the digital data was created;

means for concatenating the hash and the time data;

means for applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; and

means for encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated.

81. The encoder of claim 80, further comprising:

means for transmitting the hash to a third party for providing the time stamp and concatenating the hash and time stamp; and

means for receiving the second hash from the third party prior to encryption.

82. The encoder of claim 81, wherein the trusted third party resides at an internet address and the means for transmitting and receiving is a computer capable of accessing the internet and receiving the transmitted second hash.

83. The encoder of claim 80, further comprising a semiconductor chip having a tamper resistant clock and a tamper resistant time stamping circuit, wherein the clock outputs the time data which together with the digital signature is signed by the circuit to output the time stamp.

84. The encoder of claim ~~50~~ 47, further comprising:

a memory for storing an identifier corresponding to each of at least one user of a device which creates the digital data;

recognition means for recognizing a user of the device whose identifier is stored in the memory; and

output means for outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

85. The encoder of claim 84, wherein a private key for signing the digital data is also stored in memory corresponding to each user, wherein the identifier is inserted as associated data and the private key is used to sign the digital data.

86. The encoder of claim 84, wherein the recognition means is a fingerprint recognition system.

87. The encoder of claim 86, wherein the identifier is a name of the recognized user.

88. A decoder for authenticating digital data having an embedded digital signature in predetermined bits of the digital data, the decoder comprising:

means for extracting the digital signature from the predetermined bits;

means for decrypting the signature from the digital data resulting in a first hash;

means for applying a one-way hashing function to the digital data excluding the predetermined bits resulting in a second hash; and

means for comparing the first hash to the second hash wherein if the first hash matches the second hash the digital data is authentic.

89. The decoder of claim 88, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

90. The decoder of claim 88, wherein the digital data further comprises associated data inserted into known bits of the digital data wherein the decoder authenticates both the associated data as well as the digital data.

91. The decoder of claim 90, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

92. The decoder of claim 90, wherein the digital data is compressed using a compression standard resulting in a compressed file and wherein the digital signature is contained in a header in the compressed file, wherein the decoder further comprises:

means for decompressing the compressed file; and

means for replacing the signature from the header into the predetermined bits, prior to extracting the digital signature from the predetermined bits.

93. The decoder of claim 90, wherein the digital data is compressed using a compression standard resulting in a compressed file and wherein the digital signature and associated data are contained in a header in the compressed file, wherein the decoder further comprises:

means for decompressing the compressed file; and

means for replacing the signature and associated data from the header into the predetermined bits and the known bits, respectively, prior to extracting the digital signature from the predetermined bits.

94. A method for inserting data into digital data for subsequent authentication of the digital data, the method comprising the steps of:

receiving data from an external source;

inserting the data into the digital data; and

authenticating the digital data.

95. The method of claim 94, wherein the external source is a radio frequency transmission.

96. The method of claim 94, wherein the external source is an internet link.

97. The method of claim 94, wherein the inserted data is used for authenticating information associated with the digital data.

98. A device for inserting data into a digital data for subsequent authentication of the digital data, the device comprising:

means for receiving data from an external source;

means for inserting the data into the digital image; and

means for authenticating the digital data.

99. The device of claim 98, wherein the external source is a radio frequency transmission and the means for receiving the data comprises an antenna.

100. The device of claim 98, wherein the external source is an internet link and the means for receiving the data comprises a computer capable of accessing the internet and receiving the data.

101. The device of claim 98, wherein the inserted data is used for authenticating information associated with the digital data.

102. The device of claim 98, wherein the device is a digital image generation device and the digital data represents an image.

103. The device of claim 102, wherein the image generation device is selected from a group consisting of a digital camera, a digital video camera, and a digital scanner.

104. A method for inserting time data into digital data for subsequent authentication of both the time data and the digital data, the method comprising the steps of:

providing a semiconductor chip having a tamper resistant clock and a time stamping circuit;

outputting the digital signature and time data from the clock to the time stamping circuit;

signing the time data and the digital signature resulting in a time stamp; and

authenticating the digital data and the time data.

105. A device for inserting time data into digital data for subsequent authentication of both the time data and the digital data, the device comprising:

a semiconductor chip having a tamper resistant clock and a tamper resistant stamping circuit;

means for outputting the digital signature and time data from the clock to the time stamping circuit; and

means for signing the time data and the digital signature resulting in a time stamp.

106. The device of claim 105, wherein the device is a digital image generation device and the digital data represents an image.

107. The device of claim 106, wherein the image generation device is selected from a group consisting of a digital camera, a digital video camera, and a digital scanner.

108. A method for inserting data into digital data, the device comprising:

storing an identifier corresponding to each of at least one user of a device which creates the digital data;

recognizing a user of the device whose identifier is stored in the memory;

outputting the identifier corresponding to the recognized user from the memory; and inserting data corresponding to the identifier into the digital data.

109. The method of claim 108, wherein the inserted data is used for authenticating the digital data.

110. The method of claim 108, wherein the inserted data is used for authenticating information associated with the digital data.

111. The method of claim 108, wherein the identifier is a name of the recognized user.

112. A device for inserting data into digital data, the device comprising:

a memory for storing an identifier corresponding to each of at least one user of the device;

recognition means for recognizing a user of the device whose identifier is stored in the memory;

means for outputting the identifier corresponding to the recognized user from the memory; and

means for inserting data corresponding to the identifier into the digital data.

113. The device of claim 112, wherein a private key for signing the digital data is also stored in memory corresponding to each user, wherein the identifier is inserted into the digital data and the private key is used to subsequently sign the digital data.

114. The device of claim 112, wherein the recognition means is a fingerprint recognition means.

115. The device of claim 112, wherein the device is a digital image generation device and the digital data represents an image.

116. The device of claim 112, wherein the image generation device is selected from a group consisting of a digital camera, a digital video camera, and a digital scanner.

Add A4